IT-Sicherheitsaspekte industrieller Steuerungssysteme

Christian Freckmann[(1)], Ulrich Greveler[(2)]

[(1)]TÜV-IT GmbH
Bereich Informationssicherheit
Langemarckstr. 20
45141 Essen

[(2)]Hochschule Rhein-Waal
Labor für IT-Sicherheit
Friedrich-Heinrich-Allee 25
47475 Kamp-Lintfort

C.Freckmann@tuvit.de
mail@ulrich-greveler.de

Abstract: Zum automatisierten Messen, Steuern und Regeln und zur Produktionsüberwachung kommen in vielen industriellen Bereichen sogenannte Industrial Control Systems (ICS) zum Einsatz. Die Verbreitung standardisierten IT-Komponenten und die zunehmenden Vernetzungen der Systeme setzen die Systeme heute ähnlichen Gefährdungen aus wie in der klassischen Informationstechnik. Dabei haben ICS abweichende Anforderungen an die Schutzziele Verfügbarkeit, Integrität und Vertraulichkeit. Dies äußert sich beispielsweise in längeren Laufzeiten und Wartungsfenstern. Die von den Autoren gewonnenen Erfahrungen aus realen ICS-Anwendungsfällen und -Sicherheitsaudits sind in die Erstellung eines ICS-Security-Kompendiums eingeflossen, das vom Bundesamt für Sicherheit der Informationstechnik herausgegeben wird.

1 Einführung

Zum automatisierten Messen, Steuern und Regeln von Abläufen, beispielsweise zur Automation von Prozessen und zur Überwachung von großen industriellen Produktionssystemen, kommen in vielen Bereichen sogenannte Industrial Control Systems (ICS; deutsch: industrielle Steuerungssysteme, Automatisierungssysteme) zum Einsatz. Diese finden häufig Verwendung in der produzierenden Industrie und in Bereichen, die zu den kritischen Infrastrukturen gezählt werden, z. B. Energie, Chemie, Versorger, Infrastruktur-Einrichtungen.

ICS waren in der Vergangenheit physikalisch voneinander und im Hinblick auf die sie umgebende Umwelt isoliert und damit insbesondere vor äußeren Einflüssen geschützt. Aus diesem Grunde blieben IT-Sicherheitsbetrachtungen bei der Auswahl und Entwicklung der zumeist proprietären Software und Protokolle unberücksichtigt.

Die Verbreitung standardisierten IT-Komponenten und die zunehmenden Vernetzungen der Systeme setzen die Systeme heute ähnlichen Gefährdungen aus wie in der klassischen Informationstechnik., so dass die gesamte Sicherheitskonzeption von

Systemen zur Prozesssteuerung zu überdenken und der aktuellen Bedrohungslage anzupassen ist.

Abweichend zu IT-Infrastrukturen, wie wir sie aus Rechenzentren und dem Büroumfeld kennen, haben ICS spezifische Anforderungen an die Schutzziele Verfügbarkeit, Integrität und Vertraulichkeit. Augenfällig sind hier beispielsweise erheblich längere Gesamtlaufzeiten, die Nichtberücksichtigung automatisierter Systemupdates und eine sehr geringe Zahl von Wartungsfenstern. Aus diesen Gründen und aufgrund von Echtzeitanforderungen und Gewährleistungsansprüchen sind etablierte Schutzmaßnahmen aus dem Büroumfeld, wie der IT-Grundschutz für den normalen Schutzbedarf, nur bedingt übertragbar.

2 Vorfälle aus jüngerer Zeit, Angreiferstrukturen

Wir führen einige in der jüngeren Vergangenheit bekannt gewordenen Vorfälle auf, um die Bedrohungslage von ICS zu illustrieren.

Aurora-Projekt Idaho (2007): Im Rahmen des von der Idaho National Laboratories durchgeführten Projekts wurden ICS-Sicherheitseigenschaften mit kontrollierten Experimenten untersucht: Die Ventilsysteme einer Anlage bestehend aus Dieselgeneratoren eines Energieversorgers konnten von den (hier im staatlichen Auftrag handelnden) Angreifern so weit desynchronisiert werden, dass eine Verpuffung einen der Generatoren zerstörte. [CNN 2011]

Sobig-Amtrak (2009): Der Sobig-Virus befiel Systeme mit Microsoft-Betriebssystem, die im CSX-Hauptquartier in Jacksonville (Florida) für die Steuerung der Signalisierung von Amtrak-Eisenbahnzügen eingesetzt wurden. Für Teile des Netzes war damit die Signalisierungsfunktion außer Betrieb, so dass einige Züge für mehrere Stunden gestoppt werden mussten. [CBS 2009]

Stuxnet (2010) ist eine Malware, die im Juni 2010 öffentlich bekannt wurde und speziell Systeme befällt, die zur Überwachung von Siemens-Simatic-S7-Steuerungen eingesetzt werden. Stuxnet griff dabei in die Steuerung von Frequenzumrichtern der Hersteller Vacon und Fararo Paya ein, wodurch insbesondere die Leittechnik der Urananreicherungsanlage in Natanz, Iran, beeinflusst wurde. [ISIS 2010]

Hackereinbruch bei Telvent (2012): Der Hersteller von ICS für den Einsatz in Smart Grids gab im September 2012 bekannt, dass es Hackern gelungen ist, in das Firmennetz einzubrechen und Zugriff auf ICS-Projektdateien zu gelangen. Unter anderem war davon das OASyS-DNA-System betroffen, das Telemetriedatenaustausch und Kontrollfunktionen für Energieversorgungsnetze bereitstellt aber auch beim Betrieb von Öl- und Gaspipelines zum Einsatz kommt. [WIRED 2012]

Systematische behördliche und wissenschaftliche Unterscheidungen (vgl. [GAO 2004], [GAO 2005], [EPSR 2011] und [BSI Expo 2012]), die auf beobachteten Straftaten

basierten und Motivationen der Täter kategorisierten, zeigen grobe Täterschichtungen auf, die in Tabelle 1 zusammengefasst sind.

Tätergruppe	***Vorgehensweise / Motivation***
Cyber-Kleinkriminelle	Monetäres Interesse; keine Fokussierung auf besondere Industriebereiche
Ausländische Dienste	Nutzung von aufwändigen Werkzeugen; Informationsbeschaffung allgemein; Industriespionage
(kriminelle) Hacker, „Scriptkiddies“	Interesse unterschiedlich: Demonstration von besonderen Fähigkeiten; Prahlerei innerhalb einer Peer Group; Ausprobieren von Angriffswerkzeugen bei weniger versierten Tätern ohne konkretes Ziel; gezielte Imageschädigung von Großunternehmen
(politische) Hacker, „Hacktivisten“	politisches Interesse; Bekanntmachung einer Botschaft; öffentlichkeitswirksame Angriffe bzw. Einbrüche werden bevorzugt; oft stehen eher Webserver als produktive Systeme der Industrieunternehmen im Vordergrund, da diese Angriffe stärker wahrgenommen werden
Informationskrieg Infowar	Gezielter Angriff auf kritische Infrastruktur seitens eines Staates bzw. einer regierungsnahen Organisation; Unterbrechung der Versorgung mit Elektrizität, Wasser, Gas oder Verkehrs- und Kommunikationsdiensten (Telefonie, Internet, Funknetze); Sabotage militärischer Anlagen oder Kommunikationssysteme
Insider	Aktive oder ehemalige Mitarbeiter oder Lieferanten, die sich aggressiv gegenüber dem Unternehmen verhalten und unter Nutzung von Interna Sabotage initiieren oder Informationen stehlen; oft Einzeltäter mit beträchtlichem Schadenspotential
Autoren von Malware	Überschneidet sich teilweise mit kriminellen Gruppen (z. B. Verschlüsselungstrojaner); betrifft aber auch unspezifisch erstellte Malware bzw. Computer-Viren, die ICS-Systeme befallen
Terroristen	Zerstörung bzw. Unbrauchbarmachung kritischer Infrastrukturen; Gefährdung nationaler Sicherheit; Gefährdung von Menschenleben bis hin zu Massenmorden; Schädigung von Umwelt und Wirtschaft; Verbreitung von Angst und Schrecken
Industriespione	Stehlen von Entwurfsunterlagen, Know-how und Angebotskalkulationen im Auftrag von Diensten oder Konkurrenten oder mit dem Ziel, die erbeuteten Informationen an Letztgenannte zu verkaufen

Tabelle 1: Angreiferstrukturen

3. Beobachtungen bei ICS-Sicherheits-Audits

In der Tabelle 2 sind beispielhaft typische, in jüngerer Vergangenheit bei ICS-Sicherheits-Audits unter Mitwirkung der Autoren festgestellte Beobachtungen aufgeführt, welche Rückschlüsse auf die aktuelle Gefährdungslage in deutschen Industriebetrieben zulassen.

Komponente	***Sicherheitsrelevante Beobachtungen***	***Branche***
Netz	• Anbindung unbekannter Systeme zur Datensicherung	Energieversorger
Firewall/Router	• Regeln nicht restriktiv • undokumentierte Regeleinträge • nicht mehr benötigte Datenflüsse • Bypass im Routing • IP-Forwarding auf Servern	Chemie Automobilzulieferer Maschinenbau
Modems	• ungeschützter Zugang • Anschluss nicht dokumentiert • ständige Verbindung	Energieerzeuger
Fernwartung	• Anschluss direkt in Feldebene	Wasserversorgung Chemie
Betriebssysteme/ Härtung	• Betriebssystemkomponenten nicht gehärtet • ungenutzte Dienste angeboten • Nicht-unterstütze Version und fehlende Patches	Netzbetrieb (Energie) Maschinenbau Windpark
Funkverbin-dungen	• fehlende Verschlüsselung • veraltete Netzelemente	Öl/Gas-Industrie
Industrie-Switche	• fehlende Robustheit gegen unerwartete Kommunikation	Öl/Gas-Industrie Energieversorger
veraltete Netzelemente	• Administrativer, webbasierter Zugang ohne Absicherung • Fehlende Protokollunterstützung (z. B. nur 'telnet'-Zugang)	Automobilzulieferer Pharma

Tabelle 2: Ausgewählte Audit-Beobachtungen

Eine Auswertung dieser Audit-Ergebnisse legt den Schluss nahe, dass die festgestellten Schwachstellen unabhängig von Industriezweigen verbreitet sind und eher aufgrund einer allgemeinen Verbreitung von Standard-IT-Komponenten innerhalb von Produktionslandschaften Einzug in die Steuer- und Kontrollsysteme gehalten haben.

4. Besondere Angriffsvektoren, die im ICS-Umfeld verwendet werden

Die im Folgenden benannten Angriffsvektoren und Szenarien stellen typische Kombination von Angriffstechniken und Schwachstellen dar, die im ICS-Umfeld eine Rolle spielen. Hier werden für den Angreifer Erfolg versprechende und damit praktisch relevante Kombinationen von Schwachstellen und Techniken zur Ausnutzung von Schwachstellen in ICS-Umgebungen benannt.

Malware auf Steuerungs-PC mit Durchgriff auf SPS

Zur Programmierung von SPS (speicherprogrammierbare Steuerungen) in ICS-Installationen wird gewöhnlich ein eigener Rechner mit Steuerungssoftware verwendet. Es existiert auf ICS zugeschnittene Schadsoftware, welche von einem solchen infizierten Steuerungs-PC aus unbemerkt eigene Steuerungsbefehle zur Programmierung der SPS sendet. Hierbei weicht die visualisierte Darstellung auf dem Steuerungs-PC von der tatsächlichen Programmierung der SPS ab, da die veränderten Steuerungsbefehle nicht von dem vorgesehenen Programm übermittelt, sondern vor dem Absenden durch die Schadsoftware modifiziert werden. Somit hat der Prozessingenieur keine Möglichkeit diese Abweichung zu bemerken.

Für Angreifer ist dieser Angriffsvektor besonders „wertvoll“, da hierdurch nicht nur die SPS kompromittiert und die Produktion auf eine gewünschte Weise gestört wird. Es wird gleichzeitig die Visualisierung des Steuerungszustands im Sinne des Angreifers beeinflusst. In der Folge bemerkt das Bedienpersonal die Auswirkung des Angriffs nicht, schöpft keinen Verdacht und setzt die Produktion unvermindert fort. Beeinträchtigte Systeme können dann über einen langen Zeitraum sabotiert werden, ohne dass dies bemerkt wird.

Soziale Netze und Spear-Phishing in Bezug auf das ICS-Bedienpersonal

Nutzt das ICS-Bedienpersonal öffentliche Kommunikationsplattformen im Internet wie soziale Netze (z. B. Facebook, Xing, Linkedin), so kann ein Angreifer aus scheinbar belanglosen Informationen (z. B. Facebook-Nachricht über den Schichtbeginn oder über den Leerlauf des Personals aufgrund von Produktionsstopps oder einer Störung) ggf. Rückschlüsse auf die Produktion ziehen, die für gezielte Angriffe genutzt werden können.

So lassen sich beispielsweise mithilfe von sozialen Netzen Personen identifizieren, die sich mit dem Betrieb von ICS befassen. Daraufhin kann ein Angreifer nun gezielt Informationen über dieses ICS-Personal abrufen und dafür nutzen, um zugeschnittene Phishing-Angriffe (siehe Kapitel 3.3.2.6) auf einen kleinen Kreis oder nur eine Person

durchzuführen. Diese Phishing-Angriffe mittels gezielter Informationsbeschaffung werden als Spear-Phishing bezeichnet.

Während ursprüngliche Phishing-Attacken z. B. über massenversendete Emails aufgrund eines allgemeinen Sicherheitsbewusstseins an Bedeutung verlieren ([Vi2011], [Sh2011]), können diese gezielten, mit Hintergrundinformationen angereicherten Spear-Phishing-Angriffe eine vergleichsweise hohe Erfolgsquote verzeichnen.

Beispielsweise wird der Phishing-Versuch mittels eines vermeintlichen Hinweises eines Lieferanten zur Absendung eines vorgegebenen Kommandos im Fall einer Störung nicht mehr ignoriert werden, wenn tatsächlich kurz zuvor an diesen Lieferanten eine Störungsmeldung herausgegangen ist.

Das soziale Netz kann auch von Angreifern genutzt werden, um z. B. eine Freundschaftsanfrage eines vertrauenswürdigen Kollegen vorzutäuschen und anschließend diese Vertrauensstellung auszunutzen. So kann im Namen des Kollegen eine scheinbar plausible Handlung erbittet werden (z. B. kurzzeitiges Ändern eines Passworts auf eine vorgegebene Zeichenkette für einen angeblichen Test), um den Angriff auf das System durchzuführen.

Verfälschung von Sensordaten zu Sabotagezwecken

Historisch bedingt sind die im ICS-Umfeld verwendeten Netztechnologien und Protokolle nicht unter dem Gesichtspunkt der IT-Sicherheit entwickelt worden und weisen somit häufig keine Sicherheitsmechanismen auf. Für die Übermittlung von Steuerungsdaten werden häufig entsprechend ungesicherte Netztechnologien wie Profibus und DNP eingesetzt. Daher ist der Zugang zum Bus für einen Angreifer oftmals ausreichend, um die übertragenen Daten im Klartext lesen und frei verändern zu können. Die Kommunikation wird dabei nicht zwangsläufig unterbrochen oder gestört.

Kennzeichnend ist bei diesem Angriffsvektor, dass nur eine am Bus operierende Komponente (z. B. eine SPS) kompromittiert werden muss, um die Operation aller anderen Komponenten zu stören.

So können beispielsweise Sensordaten (z. B. Füllstand, Temperatur, Druck) verfälscht werden, um Abschaltungen oder Regelungen zu verhindern und damit den Produktionsprozess zu beeinflussen. Denkbar ist auch das Verfälschen von Produktionsparametern (z. B. Frequenzen, Umdrehungen, Dauer eines Schweißvorgangs), um gezielt Fehlproduktionen zu verursachen. Unter Umständen werden die falschen Produktionsparameter erst bei der Qualitätskontrolle bemerkt, da in der Visualisierung die dargestellten Parameter nicht mit den tatsächlich eingestellten Parametern durch den Angreifer übereinstimmen.

Darüber hinaus lassen sich ggf. Safety-Mechanismen zur wirkungsvollen Verhinderung einer Sabotage (z. B. Selbstabschaltung bei Überschreitung eines Drucks oder Unterschreitung eines Füllstandes) umgehen.

Physischer Angriff zur Provokation administrativer Eingriffe

Je nach Einsatzfeld der ICS-Installation kann ein Angreifer eine der Komponenten (z. B. externer Sensor oder Aktor) physisch manipulieren, um eine Reaktion der Bedienmannschaft zu provozieren. Auf diese Weise kann ein Angreifer gewisse Aktionen wie die Durchführung von administrativen Tätigkeiten beeinflussen und dann beispielsweise für weiterführende Angriffe nutzen.

So kann z. B. ein Temperatursensor erhitzt werden, um einen Alarm auszulösen und in der Folge eine gewisse Reaktion des Bedienpersonals hervorzurufen. Dies ist beispielsweise dann möglich, wenn der Angreifer annehmen kann, dass ein Wartungszugriff erfolgt, bei dem ein Passwort unsicher übertragen wird (Mitschneiden des Passwortes an einer Netzkomponente), ein Steuerbefehl (z. B. Neustart oder Schnellabschaltung) abgesetzt wird, den er für einen späteren Replay-Angriff benötigt oder ein ungesicherter Fernwartungszugang aktiviert wird, weil die provozierte Störung das Eingreifen eines Lieferanten-Mitarbeiters erfordert und er diesen Zugang dann für sich selbst nutzen kann.

Der Angriffsvektor kombiniert daher das Wissen über das produktive System selbst mit vorhandenen Schwachstellen von ICS-Komponenten.

Eine ähnliche Vorgehensweise stellt die ständige Alarmierung dar. Der Angreifer löst wiederholt eine Alarmierung aus (z. B. Unterbrechung einer Lichtschranke). Kommt es mehrfach zu einem administrativen Eingriff ohne eine Ursache identifizieren zu können, so wird ggf. vom Bedienpersonal von einer Fehlalarmierung ausgegangen und der Alarm bis auf weiteres deaktiviert. Auf diese Weise kann der eigentliche Angriff vorbereitet werden, der denselben Alarm auslösen würde.

5. Das ICS-Security-Kompendium

Die von den Autoren gewonnenen Erfahrungen aus realen ICS-Anwendungsfällen und ICS-Sicherheitsaudits sind in die Erstellung eines Kompendiums eingeflossen, das als Handreichung für mit der Sicherheit von ICS befassten Personen mit unterschiedlichen fachlichen Hintergründen dienen soll und auf dessen Grundlage Verbände und Organisationen spezifische Sicherheitsanforderungen erarbeiten können..

Das vom Bundesamt für Sicherheit in der Informationstechnik herausgegebene Kompendium [BSI13] richtet sich primär an Unternehmen und Personen, die ICS einsetzen. Es werden Grundlagen über die IT-Sicherheit von Automatisierungssystemen vermittelt und Vorgehen beschrieben, das IT-Sicherheitsniveau dieser ICS zu optimieren. Eine weitere Zielgruppe sind Unternehmen und Personen, welche die IT-Sicherheit von Automatisierungssystemen prüfen und bewerten. Zudem soll sie als Anregung für alle Personen dienen, die sich in irgendeiner Weise mit der IT-Sicherheit von Automatisierungssystemen beschäftigen.

Im Kompendium wird eine fundierte Einführung in die Grundlagen von ICS gegeben und die sicherheitsspezifischen Grundlagen von ICS werden erläutert. Neben der allgemeinen Einführung in Schwachstellen und Angriffsvektoren erfolgt eine Erläuterung der Besonderheiten von ICS, die an ICS-Anwender und IT-Sicherheitsexperten gerichtet ist.

Ein weiteres Kapitel gibt einen Überblick über nationale und internationale Organisationen und deren Standards und Quasi-Standards im Bereich der ICS-Sicherheit. Zudem werden architekturelle, technische und organisatorische Maßnahmen zum Schutz von ICS definiert und es erfolgt eine Gegenüberstellung der Best Practices zu etablierten Standards wie IEC 62443 und VDI/VDE 2182. Die Best Practices adressieren in erster Linie Betreiber von ICS.

Schließlich wird im Kompendium eine Methodik für die Durchführung von Audits in ICS beschrieben und aktuelle Trend aus dem ICS-Umfeld betrachtet.

Literaturverzeichnis

[BSI Expo 2012] Bundesamt für Sicherheit in der Informationstechnik: Cyber-Sicherheits-Exposition, Version 1.00, 15.10.2012 (S. 2)

[BSI13] Freckmann, Greveler et al.: ICS-Security-Kompendium. Bundesamt für Sicherheit in der Informationstechnik, 2013.

[CNN 2011] Ahlers, Mike M.: Inside a government computer attack exercise, http://edition.cnn.com/2011/10/17/tech/innovation/cyberattack-exercise-idaho/index.html, abgerufen am 10.05.2013

[CBS 2009] Niland, Marty: Virus Disrupts Train Signals, http://www.cbsnews.com/2100-205_162-569418.html, abgerufen am 10.05.2013

[EPSR 2011] Fovinoa, Igor Nai et al.: Cyber security assessment of a power plant, Electric Power Systems Research 81, 2011 (S. 518-526)

[GAO 2004] Government Accountability Office: Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems (GAO-04-628T), http://www.gao.gov/assets/120/110816.pdf, abgerufen am 13.05.2013

[GAO 2005] Government Accountability Office: Critical Infrastructure Protection: Department of Homeland Security Faces Challenges in Fulfilling Cybersecurity Responsibilities, http://www.gao.gov/assets/250/246516.pdf, abgerufen am 13.05.2013

[ISIS 2010] Albright, David; Brannan, Paul; Walrond, Christina: Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?, http://isis-online.org/uploads/isis-reports/documents/stuxnet_FEP_22Dec2010.pdf, abgerufen am 10.05.2013

[WIRED 2012] Zetter, Kim: Maker of Smart-Grid Control Software Hacked, http://www.wired.com/threatlevel/2012/09/scada-vendor-telvent-hacked/, abgerufen am 10.05.2013

[Vi2011] Vishwanatha et al.: Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. Decision Support Systems, Volume 51, Issue 3, June 2011, p. 576–586

[Sh2011] Shashidhar, Chen: A phishing model and its applications to evaluating phishing attacks. Proceedings of the 2nd International Cyber Resilience Conference 2011. p. 63-69